(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 19 805 A 1**

(51) Int. Cl.[6]:
G 07 C 11/00
G 07 C 9/00
G 06 F 12/14

(21) Aktenzeichen: P 44 19 805.1
(22) Anmeldetag: 6. 6. 94
(43) Offenlegungstag: 7. 12. 95

DE 44 19 805 A1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(74) Vertreter:
Klunker und Kollegen, 80797 München

(72) Erfinder:
Lamla, Michael, 80935 München, DE; Rankl, Wolfgang, 81677 München, DE; Weikmann, Franz, Dr., 81675 München, DE; Effing, Wolfgang, 82205 Gilching, DE

(54) Verfahren zur Echtheitsprüfung eines Datenträgers

(57) Verfahren zur Echtheitsprüfung eines Datenträgers, der wenigstens einen integrierten Schaltkreis mit Speichereinheiten und Logikeinheiten sowie eine Datenleitung zum Datenaustausch mit einer externen Einrichtung aufweist. Die Erfindung zeichnet sich dadurch aus, daß der integrierte Schaltkreis zusätzlich eine separate fest verdrahtete Schaltung zum Senden und/oder Empfangen von Daten während der Einschaltsequenz aufweist, die zur Echtheitsprüfung verwendet wird, wobei das erste Senden bzw. Empfangen der Daten innerhalb eines definierten Zeitbereichs der Einschaltsequenz abgeschlossen ist, in der die Datenleitung keinen definierten Zustand aufweist.

DE 44 19 805 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 10. 95 508 049/469

Beschreibung

Die Erfindung betrifft ein Verfahren zur Prüfung der Echtheit eines Datenträgers gemäß dem Oberbegriff des Anspruchs 1. Ferner betrifft die Erfindung eine Datenträgeranordnung zur Durchführung des Verfahrens.

Ein Verfahren zur Echtheitsprüfung ist z. B. aus der EP-A1 0 321 728 bekannt. Bei dem bekannten Verfahren wird der Datenträger durch ein von einer externen Einrichtung gesendetes Steuersignal von dem Normalbetrieb in den Kontrollbetrieb, in dem die Echtheitsprüfung erfolgt, umgeschaltet. Zu diesem Zweck besitzt der Datenträger eine zusätzliche Schaltlogik, die in Abhängigkeit von dem externen Signal diese Umschaltung vornimmt. Im Kontrollbetrieb werden dann dem Datenträger von außen Kontrolldaten zugeführt, die dann von einer zusätzlichen elektronischen Schaltung, z. B. in Form eines Analogrechners, bearbeitet werden. Die Bearbeitungszeit der Kontrolldaten durch den Analogrechner stellt hierbei ein Echtheitsmerkmal für den Datenträger dar. Bei dem bekannten Verfahren wird die in dem Kontrollbetrieb des Datenträgers stattfindende Echtheitsprüfung von dem Normalbetrieb entkoppelt, damit der Normalbetrieb, der in der Regel nach standardisierten Protokollen abläuft, nicht durch die Echtheitsprüfung gestört wird. Das bedeutet jedoch, daß vor jeder Echtheitsprüfung ein Umschalten mittels der zusätzlichen Schaltlogik vom Normalbetrieb in den Kontrollbetrieb notwendig ist.

Die Aufgabe der Erfindung besteht nun darin, ein Verfahren zur Echtheitsprüfung eines Datenträgers vorzuschlagen, bei dem die Echtheitsprüfung kompatibel mit den bereits bestehenden standardisierten Protokollen ist und mit geringem schaltungstechnischen Aufwand erfolgen kann.

Die Aufgabe wird durch die im Anspruch 1 angegebenen Merkmale gelöst.

Der Grundgedanke der Erfindung besteht darin, daß das erste Senden bzw. Empfangen der zur Echtheitsprüfung verwendeten Daten während der Einschaltsequenz für den Datenträger stattfindet, in der die Datenleitung für den Datenaustausch mit einer externen Einrichtung noch keinen definierten Zustand aufweist. Beispielsweise kann gemäß der Norm ISO/IEC 7816-3 die Datenleitung für einen definierten Zeitbereich während der Einschaltsequenz sich in einem undefinierten Zustand befinden. Da das erste Senden bzw. Empfangen der Daten innerhalb des durch die Norm definierten Zeitbereichs abgeschlossen ist, wird der für die Kommunikation mit Chipkarten standardisierte Datenaustausch nicht gestört. Dadurch kann das Prüfverfahren gemäß der Erfindung standardkonform mit bereits bestehenden Protokollen ablaufen.

Der Datenträger verfügt über eine zusätzliche spezielle Schaltung, die innerhalb des besagten Zeitbereichs, für den die Datenleitung keinen durch das Protokoll definierten Zustand aufweisen muß, die zur Echtheitsprüfung benötigten Daten an eine externe Einrichtung sendet bzw. von dieser empfängt.

In einer ersten Ausführungsform kann z. B. eine in Hardware realisierte Kennung des Datenträgers innerhalb des besagten Zeitbereichs an die externe Einrichtung übertragen werden. Die externe Einrichtung, z. B. das Kartenlesegerät, verfügt ebenfalls über eine spezielle Schaltung, die ein Empfangen der von der Karte gesendeten Daten innerhalb dieses Zeitbereichs ermöglicht, damit das Gerät die Echtheitsprüfung durchführen kann. Aber auch für den Fall, daß das Gerät keine solche spezielle Schaltung aufweist und somit nicht in der Lage ist, innerhalb der besagten Zeitdauer die von der Karte gesendeten Daten zu empfangen, wird das Kommunikationsprotokoll durch das Senden der Daten nicht gestört. Dadurch können keine Fehler im Protokollablauf auftreten, wenn die Karte mit einem herkömmlichen Gerät innerhalb dieser Zeitdauer kommuniziert.

Gemäß einer Weiterbildung kann die auf dem integrierten Schaltkreis des Datenträgers befindliche spezielle Schaltung innerhalb des besagten Zeitbereichs auch eine Zufallszahl generieren, die dann von der speziellen Schaltungslogik des Datenträgers mit der Kennung des Datenträgers logisch verknüpft wird, wobei das Ergebnis der Verknüpfung innerhalb des besagten Zeitbereiches, jedoch spätestens im Answer-To-Reset-Signal (ATR) vom Datenträger an die externe Einrichtung übertragen wird. Durch die Verwendung einer Zufallszahl wird ein Replayangriff, d. h. die Wiedereinspielung der zuvor gesendeten Daten, unmöglich gemacht.

In einer weiteren Ausführungsform kann auch die externe Einrichtung, z. B. das Kartenlesegerät, eine zusätzliche Schaltung aufweisen, die zur Erzeugung der Zufallszahl dient. Die Zufallszahl wird dann vorzugsweise wegen der höheren Übertragungsgeschwindigkeit synchron zum Taktsignal innerhalb des besagten Zeitbereiches an den Datenträger gesendet. Die spezielle zusätzliche Schaltung des Datenträgers ist in der Lage, die gesendete Zufallszahl innerhalb des besagten Zeitbereichs, für den das Kontaktelement keinen definierten Zustand aufweisen muß, zu empfangen und zumindest einen Teil der empfangenen Zufallszahl innerhalb dieser Zeit wieder an die externe Einrichtung zurückzusenden. In Erweiterung hierzu kann die spezielle Schaltungslogik des Datenträgers auch die empfangene Zufallszahl mit der Kennung des Datenträgers logisch verknüpfen und das Ergebnis der Verknüpfung als Bestätigung für den Empfang der Zufallszahl innerhalb des besagten Zeitbereichs oder spätestens jedoch im ATR-Signal an die externe Einrichtung zurücksenden. Die externe Einrichtung kann dann anhand des von dem Datenträger empfangenen Ergebnisses der Verknüpfung nachprüfen, ob der Datenträger nachweislich fähig ist, innerhalb des besagten Zeitbereichs die gesendete Zufallszahl zu empfangen und richtig mit der Kennung des Datenträgers innerhalb einer vorbestimmten Zeit zu verknüpfen und an die externe Einrichtung zu übertragen. Das Vorhandensein des Ergebnisses der Verknüpfung im ATR-Signal stellt hierbei eine Klassenkennung für den Datenträger dar und kann als solche von der externen Einrichtung ausgewertet werden, wohingegen der Inhalt des Ergebnisses der Verknüpfung eine für den Datenträger individuelle Kennung darstellt.

Weitere Vorteile und vorteilhafte Weiterbildungen sind der Beschreibung der Erfindung anhand der Figuren entnehmbar.

Die Figuren zeigen:

Fig. 1 eine Datenträgeranordnung zur Echtheitsprüfung,

Fig. 2 den standardisierten Signalverlauf bei der Einschaltsequenz des Datenträgers,

Fig. 3a—3c ein Ausführungsbeispiel des erfindungsgemäßen Prüfverfahrens, bei dem der Datenträger die Daten sendet,

Fig. 4 und 5 jeweils ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens, bei dem die Daten von einer externen Einrichtung gesendet und vom Datenträger empfangen werden,

Fig. 6 ein Prinzipschaltbild des Datenträgers,

Fig. 7 ein Ausführungsbeispiel einer speziellen Schaltung,

Fig. 8 ein weiteres Ausführungsbeispiel einer speziellen Schaltung des Datenträgers.

Fig. 1 zeigt eine Datenträgeranordnung zur Echtheitsprüfung eines Datenträgers in Form einer Chipkarte 1, die über eine Datenleitung 4 mit einer externen Einrichtung 5, z. B. Kartenlesegerät, kommuniziert.

Fig. 2 zeigt den Signalverlauf beim Reset des Datenträgers, wie er z. B. im internationalen Standard ISO/IEC 7816-3 genormt ist. Im einzelnen sind dies das Massepotential GND, die Versorgungsspannung VCC, das zum Rücksetzen des Datenträgers extern zugeführte Reset-Signal RST, das Taktsignal CLK und die Datenleitung I/O. Bei anliegender Versorgungsspannung und Stabilisierung der Spannung und Anliegen des Taktsignales zum Zeitpunkt T_0 befindet sich die Datenleitung I/O im Empfangsmodus für das von einer externen Einrichtung zum Zeitpunkt T_1 gelieferte Reset-Signal RST. Ab dem Zeitpunkt T_0 kann die Datenleitung I/O gemäß der besagten Norm für den Zeitbereich t_2 sich in einem undefinierten Zustand befinden. Entsprechend der Norm muß dieser Zeitbereich t_2 kleiner gleich 200 Taktzyklen, dividiert durch die Taktfrequenz f_i sein. Nach Verstreichen dieser Zeitdauer muß sich die Datenleitung I/O in einem definierten Zustand befinden und kann daher nicht zum Senden bzw. Empfangen von Daten vor dem Reset-Signal RST verwendet werden. Mit dem Empfang des Reset-Signals RST zum Zeitpunkt T_1 antwortet der Datenträger nach der Zeitdauer t_1 mit dem Answer-To-Reset-Signal ATR.

Fig. 3a zeigt den ersten Sendevorgang, z. B. die Übertragung einer Kennung KN, des Datenträgers von diesem an eine externe Einrichtung innerhalb des Zeitbereiches t_2. Sobald das Taktsignal CLK anliegt, überträgt der Datenträger automatisch direkt die Kennung, z. B. die Serien-Nr. vorzugsweise synchron zum Taktsignal, an die externe Einrichtung. Die synchrone Übertragung ermöglicht eine höhere Sendegeschwindigkeit gegenüber einer asynchronen Übertragung. Selbstverständlich könnte die Übertragung der Serien-Nr. auch asynchron zum Taktsignal erfolgen, wenn dies innerhalb des Zeitbereiches t_2 durchführbar ist. In jedem Fall verfügt der Datenträger hierbei zusätzlich zu den üblichen Logik- und Speichereinheiten über eine spezielle Schaltung, die dieses schnelle Senden im genannten Zeitraum ermöglicht. Mit einem Standardkommando kann dann die externe Einrichtung die in einem Speicher des Datenträgers gespeicherte Serien-Nr. auslesen und diese mit der von dem Datenträger empfangenen Serien-Nr. vergleichen. Stimmt die von dem Datenträger mittels der speziellen Schaltung gesendete und die aus dem Speicher des Datenträgers ausgelesene Serien-Nr. überein, so ist der Datenträger nachweislich fähig, sehr schnell innerhalb des Zeitbereichs von t_2 die für die Echtheitsprüfung notwendigen Daten zu senden. Diese Eigenschaft ist ein Echtheitsmerkmal, das von keinem herkömmlichen Datenträger, d. h. einem Datenträger ohne diese spezielle Schaltung, erfüllt werden kann.

Der in Fig. 3b gezeigte Verfahrensschritt stellt eine Erweiterung des Verfahrens gemäß Fig. 3a dar. Dabei wird die Kennung KN mit einer vom Datenträger generierten Zufallszahl RND, z. B. Exklusiv Oder verknüpft, wobei das Ergebnis der Verknüpfung mit der generierten Zufallszahl RND zur externen Einrichtung gesendet wird. Die Zufallszahl wird innerhalb des Zeitbereichs von t_2 erzeugt. Vorzugsweise erfolgt die Übertragung des Ergebnisses der Verknüpfung mit der Zufallszahl RND ebenfalls innerhalb der Zeitdauer von t_2. Jedoch ist es auch möglich, wie dies in Fig. 3c dargestellt ist, das Ergebnis der Verknüpfung und die Zufallszahl im Answer-To-Reset-Signal des Datenträgers z. B. in den historical characters des ATR-Signals mit zu übertragen. Die externe Einrichtung kann dann gemäß dem normalen Protokollablauf in einem späteren Authentisierungsschritt die empfangene Zufallszahl mit der aus einem Speicher des Datenträgers ausgelesenen Kennung KN nach der gleichen logischen Operation wieder verknüpfen und das Ergebnis der Verknüpfung mit dem im ATR-Signal übertragenen Ergebnis der Verknüpfung des Datenträgers vergleichen. Durch die Verwendung einer Zufallszahl wird ein Replayangriff durch Wiedereinspielung der zuvor aufgezeichneten Daten unmöglich gemacht.

Fig. 4 zeigt nun ein weiteres Ausführungsbeispiel des erfindungsgemäßen Verfahrens. In einem ersten Verfahrensschritt sendet die externe Einrichtung innerhalb des Zeitraums t_2 eine Zufallszahl RND, die z. B. 8 Byte umfassen kann, an den Datenträger. Die Übertragung erfolgt vorzugsweise synchron zum Taktsignal, kann jedoch auch asynchron erfolgen. Innerhalb der Zeitdauer t_2 sendet der Datenträger wenigstens das letzte Byte R_8'der empfangenen Zufallszahl an die externe Einrichtung zurück. Die externe Einrichtung vergleicht daraufhin das letzte von ihr generierte Byte R_8 der Zufallszahl mit dem vom Datenträger empfangenen Byte R_8'. Stimmen diese überein, so konnte der Datenträger die gesendete Zufallszahl richtig empfangen und wenigstens einen Teil wieder zurücksenden. Die Tatsache, daß der Datenträger sehr schnell Daten empfangen kann, stellt hierbei ein Echtheitsmerkmal dar. Anstelle des letzten Bytes der Zufallszahl kann selbstverständlich der Datenträger auch die gesamte innerhalb des Zeitraums t_2 empfangene Zufallszahl wieder an die externe Einrichtung zurücksenden. Dies kann beispielsweise auch im ATR-Signal miterfolgen.

Ergänzend hierzu kann die innerhalb des Zeitraums t_2 von der externen Einrichtung empfangene Zufallszahl RND von der speziellen Schaltungslogik des Datenträgers mit der Kennung KN des Datenträgers durch eine logische Operation verknüpft werden. Als Verknüpfungsoperation kann z. B. eine Polynom-Modulo-Division mit der Kennung als Teilerpolynom für die Zufallszahl verwendet werden. Diese Verknüpfungsoperation ist dem Fachmann geläufig und wird daher hier nicht näher beschrieben. Die derart mit der Zufallszahl verknüpfte Kennung KN des Datenträgers kann dann innerhalb der Zeitdauer von t_2 oder im ATR-Signal des Datenträgers an die externe Einrichtung gesendet werden. Beide Varianten sind hier denkbar. Die externe Einrichtung erhält dann durch Ausführung einer zu der Verknüpfungsoperation inversen Funktion aus dem Ergebnis der Verknüpfung von Zufallszahl und Kennung wieder die durch den Datenträger empfangene Zufallszahl und vergleicht diese mit der von der externen Einrichtung generierten Zufallszahl. Stimmen diese überein, so zeigt dies, daß der Datenträger, insbesondere die spezielle Schaltung des Datenträgers, nachweislich fähig ist, sehr schnell die Zufallszahl zu empfangen und zu verknüpfen und das Ergebnis der Verknüpfung innerhalb von t_2 oder jedoch spätestens im ATR-Signal des Datenträgers, z. B. in den historical characters, an die externe Einrichtung zu senden.

Fig. 5 zeigt ein weiteres Ausführungsbeispiel, bei dem die von der externen Einrichtung gesendete Zufallszahl RND, die z. B. mehrere Bytes umfassen kann, innerhalb

der Zeitdauer von t_2 von dem Datenträger empfangen wird, wobei entweder die ganze Zufallszahl oder zumindest das letzte Byte der gesendeten Zufallszahl je nach Länge der Zufallszahl mit der Kennung KN des Datenträgers Exklusiv Oder verknüpft wird, wobei das Ergebnis der Verknüpfung gemeinsam mit der Kennung des Datenträgers innerhalb der Zeitdauer von t_2 oder im ATR-Signal an die externe Einrichtung übertragen wird. Die externe Einrichtung führt dann nochmals die gleiche logische Operation ausgehend von der empfangenen Kennung KN und der generierten Zufallszahl RND aus und vergleicht das von der externen Einrichtung erhaltene Ergebnis der Verknüpfung mit dem von dem Datenträger empfangenen Ergebnis der Verknüpfung.

Der in **Fig. 6** schematisch dargestellte Datenträger 1 unterscheidet sich von den herkömmlichen Datenträgern, z. B. mit einem Mikroprozessor, dadurch, daß zusätzlich zum üblichen Mikrokontroller 3 eine zusätzliche spezielle Schaltung 2 zum Senden bzw. Empfangen von Daten und einer eventuellen Verknüpfung der Daten mit einer in Hardware realisierten Kennung des Datenträgers, z. B. Serien-Nr., vorgesehen ist. Die Kennung des Datenträgers kann z. B. beim Herstellungsvorgang des integrierten Schaltkreises durch Zünden von Sicherungen als Hardware-Merkmal für die spezielle Schaltung des integrierten Schaltkreises realisiert werden. Die hardwaremäßige Realisierung einer solchen Kennung ist z. B. in der noch nicht veröffentlichten Patentanmeldung PCT/EP 93/03668 beschrieben. Ergänzend zu den in dieser Anmeldung beschriebenen Ausführungsformen kann die Kennung z. B. auch durch Setzen der Sicherungen mittels eines "Laser-Cutters" in der "Wafer-Fab" (Herstellung) erfolgen, wodurch die Sicherungen in einen definierten logischen Zustand irreversibel gesetzt werden. Der Mikrokontroller 3 des Datenträgers kann bei der gezeigten Konfiguration auch direkt auf die spezielle Schaltung 2 zugreifen, so kann z. B. der Mikrokontroller 3 das von der speziellen Schaltungslogik 2 errechnete Ergebnis der Verknüpfung dann auslesen, wenn das von der speziellen Schaltung 2 berechnete Ergebnis als ein Bestandteil des ATR-Signals, z. B. in den historical characters zur externen Einrichtung gesendet werden soll. Die spezielle Schaltung 2 kann jedoch auch ohne Mitwirkung des Mikrokontrollers 3 das Ergebnis der Verknüpfung direkt über die Datenleitung I/O an die externe Einrichtung innerhalb des Zeitbereichs von t_2 übertragen, da die spezielle Schaltung 2 direkt mit GND, VCC, Reset, Clock und der I/O-Datenleitung verbunden ist. Diese Hardware-Konfiguration des Datenträgers ermöglicht, daß das schnelle Senden bzw. Empfangen von Daten und eventuell die Verknüpfung der Daten mit einer Kennung des Datenträgers in dem genannten Zeitraum t_2 durchführbar ist. Statt der I/O-Leitung kann die spezielle Schaltung 2 auch mit einer der beiden, nicht dargestellten, RFU-Leitungen (reserve for future use) verschaltet werden. Der Einbau dieser speziellen Schaltung als Echtheitsmerkmal für einen Datenträger verhindert, daß das Echtheitsprüfverfahren durch herkömmliche Datenträger, z. B. mit Mikroprozessor, durch diesen oder durch eine externe Logikschaltung emuliert bzw. simuliert werden kann.

Fig. 7 zeigt die wesentlichen Bestandteile einer speziellen Schaltung 2 des Datenträgers, die z. B. in der Lage ist, eine Polynom-Modulo-Division der Zufallszahl mit der Kennung des Datenträgers als Teilerpolynom durchzuführen. Diese spezielle Schaltung 2 umfaßt z. B. 32 XOR, 32 AND, ein NEG-Gatter und ein Schieberegister A. Weiterhin befinden sich auf dem integrierten Schaltkreis des Datenträgers nicht dargestellte Sicherungen, die z. B. mittels eines "Laser-Cutters" in einen definierten logischen Zustand bei der Herstellung des "Wafers" gesetzt werden. Durch diese Sicherungen kann z. B. die Kennung als Hardware-Merkmal realisiert werden, wobei ein weiteres Register B die Kombination der logischen Zustände der gesetzten Sicherungen beinhaltet. Die von der externen Einrichtung gesendete Zufallszahl RND wird in das Schieberegister A geladen und mittels der Logikgatter wird eine Polynom-Modulo-Division der Bitpositionen der Zufallszahl im Register A mit dem Register B realisiert, welches durch die Kennung, z. B. Serien-Nr. des Datenträgers, bestimmt ist.

Fig. 8 zeigt ein weiteres Ausführungsbeispiel einer speziellen zusätzlichen Schaltung 2 eines Datenträgers. Bei dieser Ausführungsform wird die von der externen Einrichtung gesendete Zufallszahl RND an ein erstes Schieberegister SR1 übertragen, wobei die Kennung KN des Datenträgers in dem Register B enthalten ist. Die Kennung des Datenträgers kann z. B. aus zwei Teilen bestehen, wobei der zweite Teil eine Negierung der Bitfolgen des ersten Teils darstellt. Synchron zum Takt wird dann die Zufallszahl RND mit der Kennung, z. B. der Serien-Nr., Exklusiv Oder verknüpft. Wenn die Verknüpfung abgeschlossen ist, was mittels entsprechender Zähler festgestellt wird, wird dann das Ergebnis der Verknüpfung sowie die Kennung synchron zum Takt an das zweite Schieberegister weitergegeben und an die externe Einrichtung zurückgesendet. Dies erfolgt vorzugsweise innerhalb des Zeitbereiches von t_2.

Patentansprüche

1. Verfahren zur Echtheitsprüfung eines Datenträgers, der wenigstens einen integrierten Schaltkreis mit Speichereinheiten und Logikeinheiten aufweist und über eine Datenleitung mit einer externen Einrichtung Daten austauscht, wobei der Datenträger von der externen Einrichtung die zum Betrieb notwendigen Betriebs- und Steuersignale erhält, **dadurch gekennzeichnet,** daß der integrierte Schaltkreis zusätzlich eine separate, festverdrahtete Schaltung zum Senden und/oder Empfangen von Daten während einer gemäß einem Protokoll definierten Einschaltsequenz aufweist, die zur Echtheitsprüfung verwendet wird, wobei das erste Senden bzw. Empfangen der zur Echtheitsprüfung verwendeten Daten innerhalb eines definierten Zeitbereichs der Einschaltsequenz abgeschlossen ist, in der die Datenleitung keinen durch das Protokoll definierten Zustand aufweist.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Einschaltsequenz nach dem standardisierten Protokoll ISO/IEC 7816-3 erfolgt, wobei das erste Senden bzw. Empfangen der Daten innerhalb des durch das Protokoll definierten Zeitbereichs t_2 abgeschlossen ist.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Daten von der externen Einrichtung innerhalb des Zeitbereichs t_2 gesendet und von dem Datenträger empfangen werden, und das Zurücksenden der empfangenen Daten durch den Datenträger ebenfalls innerhalb von t_2 oder in dem vom Protokoll definierten Answer-To-Reset-Signal des Datenträgers zur externen Einrichtung erfolgt.
4. Verfahren nach Anspruch 3, dadurch gekenn-

zeichnet, daß die von der externen Einrichtung empfangenen Daten von dem Datenträger mit einer Kennung des Datenträgers verknüpft werden und das Ergebnis der Verknüpfung innerhalb des Zeitbereichs t_2 oder im Answer-To-Reset-Signal an die externe Einrichtung zurückgesendet wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Ergebnis der Verknüpfung mit der Kennung des Datenträgers von diesem an die externe Einrichtung zur Echtheitsprüfung übertragen wird.

6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die von der externen Einrichtung gesendeten Daten eine von dieser generierte Zufallszahl darstellen, die mittels einer Exklusiv-Oder-Operation mit der Kennung des Datenträgers von diesem verknüpft wird oder eine Polynom-Modulo-Division der Zufallszahl mit der Kennung als Teilerpolynom durch den Datenträger erfolgt.

7. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß der Datenträger innerhalb des Zeitbereichs t_2 an die externe Einrichtung eine Kennung des Datenträgers sendet, die anschließend von der externen Einrichtung zur Echtheitsprüfung des Datenträgers ausgewertet wird.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Kennung des Datenträgers vor dem Senden an die externe Einrichtung vom Datenträger mit einer vom Datenträger generierten Zufallszahl verknüpft wird und das Ergebnis dieser Verknüpfung an die externe Einrichtung zur Echtheitsprüfung des Datenträgers übertragen wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß das Senden der zur Echtheitsprüfung verwendeten Daten synchron mit einem von der externen Einrichtung an den Datenträger übermittelten Taktsignal erfolgt.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß die Datenübertragung bei der Echtheitsprüfung synchron mit einem Vielfachen der externen Taktfrequenz erfolgt.

11. Datenträgeranordnung zur Durchführung eines Verfahrens nach Anspruch 1 mit einem Datenträger, der wenigstens einen integrierten Schaltkreis mit Speichereinheiten und Logikeinheiten aufweist und über eine Datenleitung mit einer externen Einrichtung Daten austauscht, wobei der Datenträger durch die externe Einrichtung die zum Betrieb des Datenträgers notwendigen Betriebs- und Steuersignale erhält und die externe Einrichtung zumindest auf Teilbereiche der Speichereinheiten des Datenträgers zum Lesen und/oder Schreiben Zugriff hat, dadurch gekennzeichnet, daß der integrierte Schaltkreis zusätzlich eine separate festverdrahtete Schaltung zum Senden und/oder Empfangen von Daten während einer gemäß einem Protokoll definierten Einschaltsequenz aufweist, die zur Echtheitsprüfung verwendet wird, wobei die separate Schaltung das erste Senden bzw. Empfangen der zur Echtheitsprüfung verwendeten Daten unabhängig von den Logikeinheiten und Speichereinheiten des Datenträgers innerhalb eines definierten Zeitbereichs der Einschaltsequenz durchführt, in der die Datenleitung keinen durch das Protokoll definierten Zustand aufweist.

12. Datenträgeranordnung nach Anspruch 11, dadurch gekennzeichnet, daß die separate Schaltung eine in Hardware realisierte Kennung für den Datenträger aufweist.

13. Datenträgeranordnung nach Anspruch 12, dadurch gekennzeichnet, daß die separate Schaltung des Datenträgers innerhalb des durch das Protokoll ISO/IEC 7816-3 definierten Zeitbereichs t_2 die Kennung des Datenträgers an die externe Einrichtung überträgt.

14. Datenträgeranordnung nach Anspruch 12, dadurch gekennzeichnet, daß die separate Schaltung des Datenträgers eine Zufallszahl generiert und diese mit der Kennung des Datenträgers verknüpft.

15. Datenträgeranordnung nach Anspruch 12, dadurch gekennzeichnet, daß die separate Schaltung des Datenträgers eine von der externen Einrichtung empfangene Zufallszahl mit der Kennung des Datenträgers verknüpft.

Hierzu 4 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 44 19 805 A1
Int. Cl.[6]: G 07 C 11/00
Offenlegungstag: 7. Dezember 1995

FIG. 1

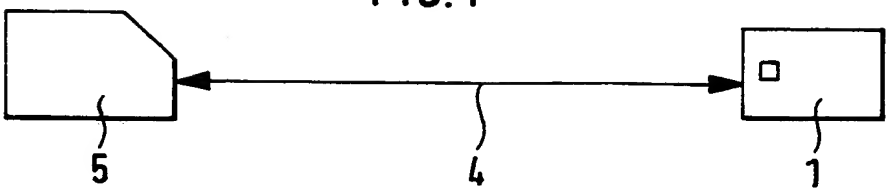


FIG. 2

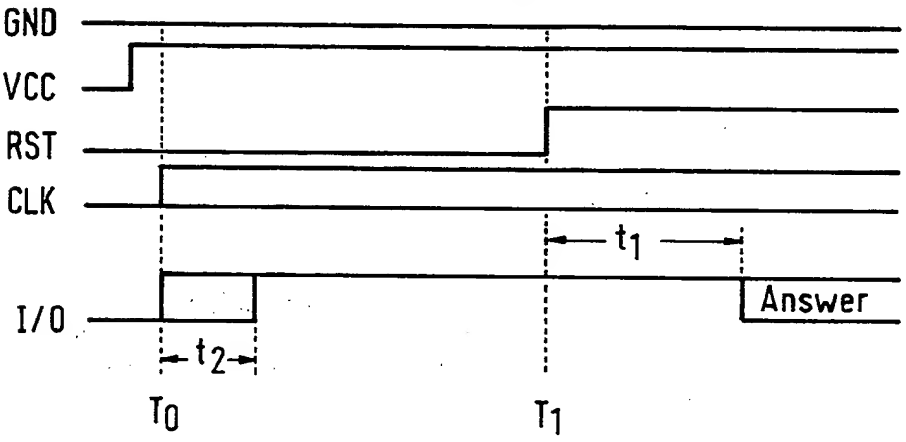


FIG. 3a

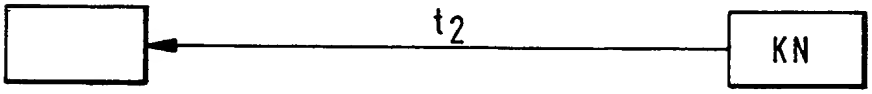


FIG. 3b

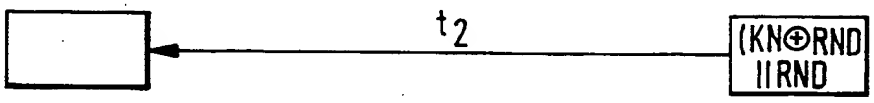


FIG. 3c

Nummer: DE 44 19 805 A1
Int. Cl.[6]: G 07 C 11/00
Offenlegungstag: 7. Dezember 1995

FIG. 4

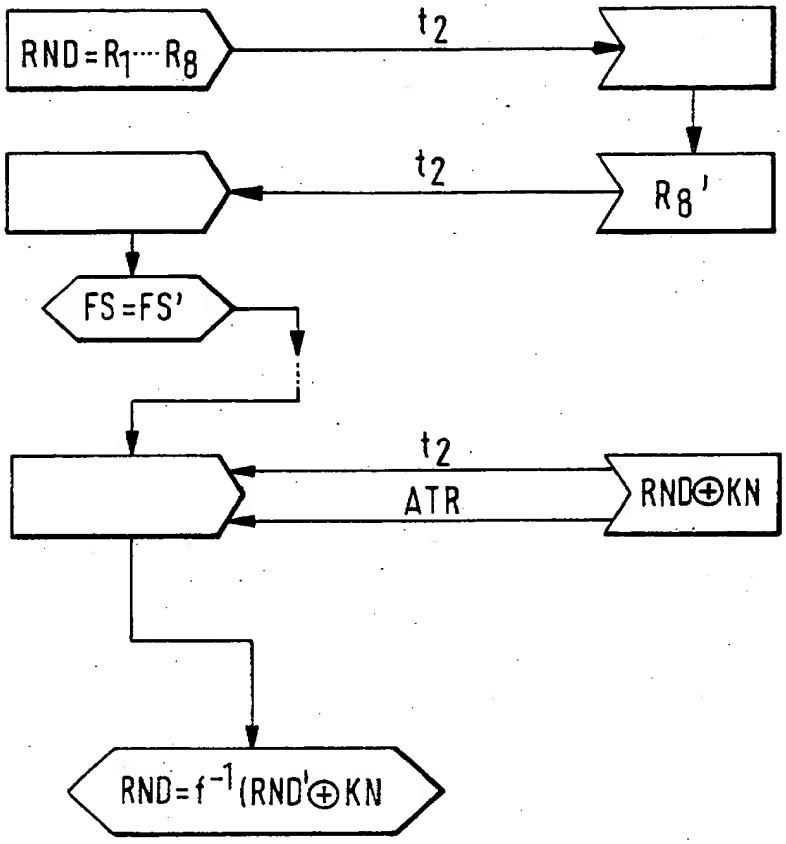
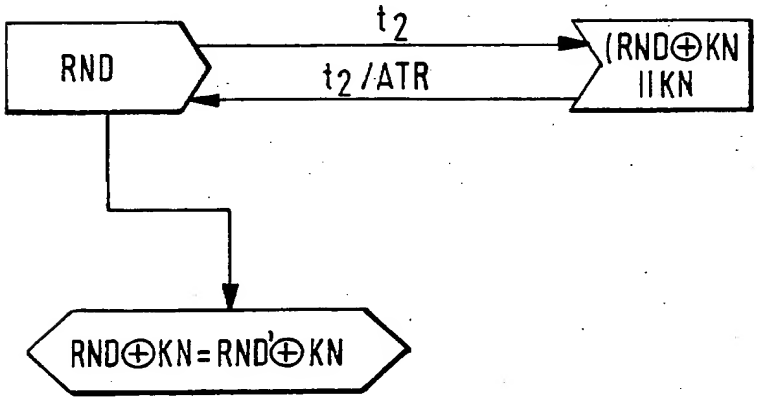


FIG. 5



Nummer: DE 44 19 806 A1
Int. Cl.[6]: G 07 C 11/00
Offenlegungstag: 7. Dezember 1995

FIG. 6

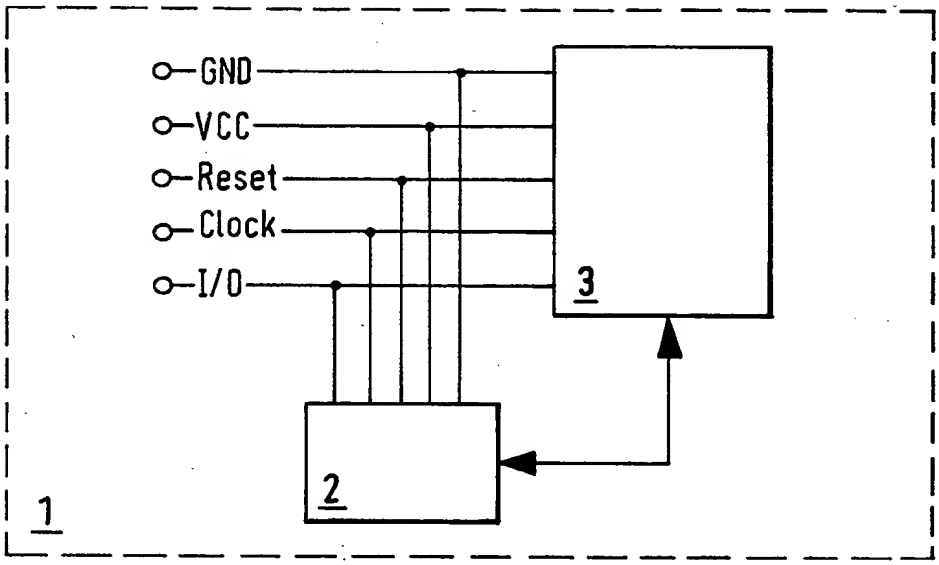
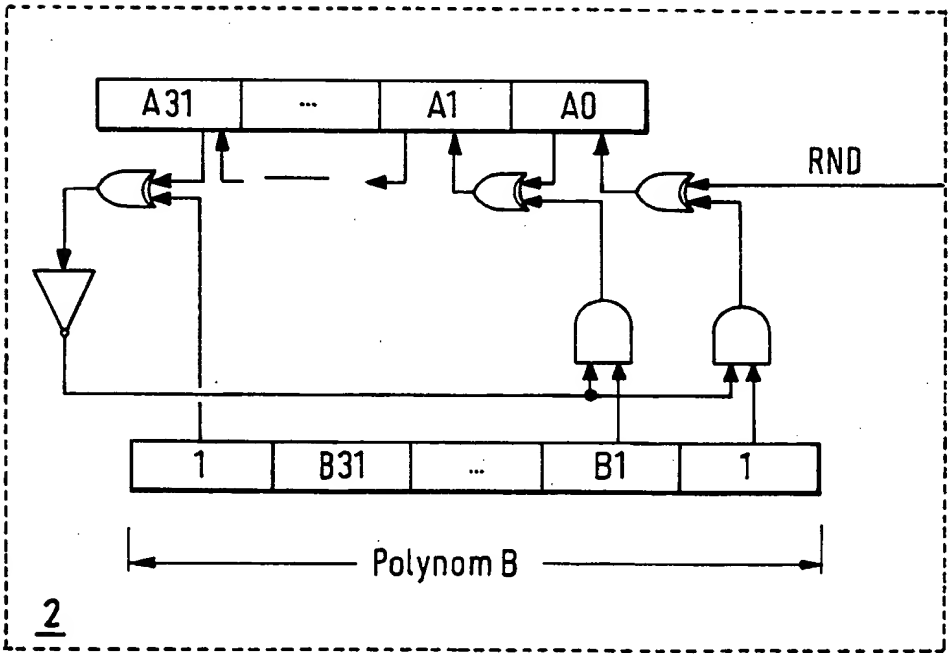


FIG. 7



Nummer: DE 44 19 805 A1
Int. Cl.[6]: G 07 C 11/00
Offenlegungstag: 7. Dezember 1995

FIG. 8